

## Exhibit D

### System.Firewall.Policy.Applicati nSetting

```
namespace System.Firewall.Policy
{
    public class ApplicationSetting
    {
        // by default, security level and trusted contacts will be set to be values returned
        // from GetDefaultSecurityLevel(user) and DefaultTrustedContacts.
        public ApplicationSetting(ApplicationID app, IPrincipal user);

        public ApplicationID Application { get { } }
        public IPrincipal User { get { } }

        public SecurityLevel SecurityLevel { get { } set { } }
        public ApplicationRuleCollection GetRules();
    }
}
```

Property	
<b>Parameters</b>	Application
<b>Description</b>	The application for which this application setting is about.
<b>Access</b>	Read Only

Property	
<b>Parameters</b>	User
<b>Description</b>	The user for which this application setting is specified. Together with the application field, it serves as the unique key for application settings.
<b>Access</b>	Read Only

Property	
<b>Parameters</b>	SecurityLevel
<b>Description</b>	The security level when this user uses this application.
<b>Access</b>	Read Write

**BEST AVAILABLE COPY**

Method	
<b>Name</b>	GetRules
<b>Parameters</b>	Application – The application to which this security level is to be applied. User – The user to which this security level is to be applied. Contacts – The list of remote contacts that is used when this security level is applied.
<b>Returns</b>	ApplicationRuleCollection
<b>Description</b>	Obtain the list of application rules that enforces the setting “using this security level with these remote contacts when this user uses this application”.

## System.Firewall.Policy.SecurityLevel

```

namespace System.Firewall.Policy
{
    public class SecurityLevel : PolicyObject
    {
        protected ApplicationRuleCollection ruleTemplates;

        public SecurityLevel(ApplicationRuleCollection ruleTemplates);

        public ApplicationRuleCollection Templates { get { } }
    }
}

```

Property	
<b>Parameters</b>	Templates
<b>Description</b>	The list of application rule templates that make of this security level.
<b>Access</b>	Read Only

The reference of remote entities in a security level determines the setting for IPSec main mode key exchange. For example, if a trusted contact is an X509 certificate, the CA certificate for this contact will be treated as a trusted root certificate used in IKE negotiation. For the security reason, certificates, pre-shared keys and other credentials

will be not stored by the PFW service. Instead the should come from the dedicated windows security stores e.g. secure certificate store for certificates.